PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06 — A1

(11) International Publication Number: **WO 00/57613**

(43) International Publication Date: 28 September 2000 (28.09.00)

(21) International Application Number: PCT/US00/07588

(22) International Filing Date: 22 March 2000 (22.03.00)

(30) Priority Data:
60/125,437 22 March 1999 (22.03.99) US

(71) Applicant *(for all designated States except US)*: MICROVAULT CORP. [US/US]; 17011 Beach Boulevard, #900, Huntington Beach, CA 92697 (US).

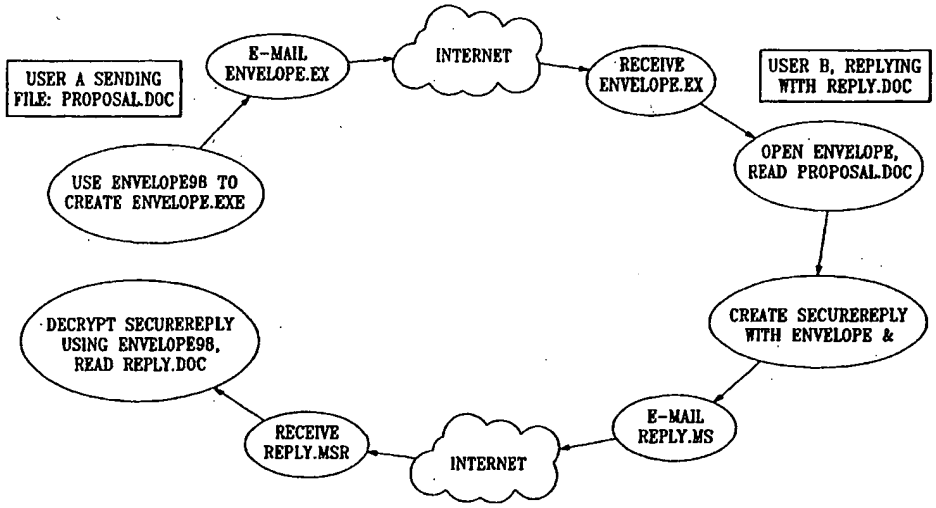
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: SHMELEV, Alexander, V. [-/US]; 992 Noria Street, Laguna Beach, CA 92651 (US).

(74) Agent: KLEINBERG, Marvin, H.; Kleinberg & Lerner, LLP, 2049 Century Park East, #1080, Los Angeles, CA 90067-3150 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR SECURE DATA TRANSMISSION SYSTEM



(57) Abstract

An apparatus and method creates a secure document with installed software at a sending location. The secure document includes an executable program which, when received and opened, runs a program that can decrypt the secure document. A pass word or phrase may be included to prevent unauthorized access to the secure document. A secure reply option may be provided which, if selected, permits the received program to encrypt a reply and to transmit the encrypted reply to the sending location. The installed software can then open the reply. In alternative embodiments, the executable program contacts a predetermined global computer network site which provides a program to decrypt the secure message. Further, the executable program and/or the program downloaded from the site enables communication with a second global computer network site which can be instructed to take a particular selected action. A confirmation can be returned to the sending location, either from the receiving location or from the second global computer network site.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD AND APPARATUS FOR SECURE DATA TRANSMISSION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to data transmission systems and, more particularly, a method and apparatus for transmitting a secure document so that a recipient can review the document and provide a secure response without special apparatus at the receiving end.

2. Description of the Related Art

Most secure data systems of the prior art have required special equipment at both the transmission and reception ends in order to recover the secure information and provide a secure reply. Such systems usually include encryption and decryption devices at both ends of a message.

Clearly, the sender must have apparatus for converting plain text into some encrypted or encoded format that is illegible to anyone lacking compatible apparatus at the receiving end. With so many different types and styles of encryption and encoding in an attempt to achieve secure communications, and in the absence of a single, standard system, the probability is low that the sender and receiver will have compatible encryption systems.

The Internet (global computer network) is a fast growing medium for information exchange. Although much of this information is of dubious value, the usefulness of the Internet as a vehicle for electronic commerce means that there is an increasing need to provide security for data transmissions.

Different types of data transmissions present different risks and obstacles and require suitable protection from tampering, corruption, theft, unauthorized access, etc. Many software and hardware products that provide such security for Internet data require that users at both ends of the transaction (i.e. sender and receiver) have the same software components or at least a highly compatible set.

This requirement for having nearly identical software at both ends of a data exchange is highly limiting. Imagine an exchange that involves parties from five different organizations! This requirement can be (and has been) dealt with by products such as Norton Secret Stuff from Symantec, Zip and WinZip from PKWare, Universal Envelope from VIAexpress, and Envelope98 from the assignee of the present invention. Each product "wraps" the message to be transmitted in an "electronic envelope". This "envelope" contains all the computer code and logic necessary to protect the message during transmission and to extract it at the receiving end.

Such an "envelope" can successfully protect data sent to a receiver.

However, in many cases the receiver may want (or be required) to reply and the reply must also be protected during transmission. Here again, a problem reoccurs. The receiver is required to install and use some type of cryptographic software or hardware to protect the reply.

Most importantly, this problem must be solved in a way that is simple to use and doesn't require an excessive amount of preparation (i.e. creating and distributing certificates and public keys, maintaining a authentication chain and a public key ring). Generally, in each case where it is necessary to transmit data securely and bidirectionally between two entities (either directly or through a private or public communication system) identical or highly compatible software and/or hardware must be installed at both ends. This presents difficulties whenever a party wishes to exchange information with more than one other party. Even then, it may be difficult to assure that both parties have equipment capable of communicating with each other.

Many products and technologies exist that can solve the problem. These include technologies known as PGP ("pretty good privacy"), PEM, S/MIME and SSL. In each case the systems are not cross-compatible (i.e. a message encrypted using the PGP system cannot by decrypted using S/MIME and vice versa). In addition, users of these systems are forced into a complicated series of operations to prepare for a data exchange (i.e. key generation, authenticity certification, etc.). Several systems require the participation of a trusted third party to authenticate the identity of the parties participating in the data transfer.

Although the existing systems are useful in certain situations, their acceptance has been slow and limited due to the high costs (in the form of computer resources and user time) and limited cross-compatibility.

For example, if two users from the same organization wish to communicate using PGP, they would exchange public keys using a central computer (authentication/key server). Such a server would, in essence, guarantee to each user the identity of the other as well as providing to each the other's encryption keys. Because most organizations would select a single system to use for secure information exchange (i.e. PGP), the users could now exchange e-mail easily and securely.

If however, the two users are from different organizations, there may be no central computer to use as a "certification authority". The users would then have to exchange keys in person or by mail. They could also rely on a trusted third party to provide this service. The two users would still have to establish a common standard with which to encrypt their data: PGP, PEM, S/MIME, etc. One or both might have to switch to this agreed upon

standard.

It quickly becomes obvious that the overhead created during this process greatly complicates the needed exchanges. If the exchange is between more than two users belonging to more than two organizations, the level of complexity increases rapidly. A simpler solution is required.

Two users, both with "electronic envelope" software, could exchange information without first agreeing on a standard system. However, each would have to install into their computer some form of electronic envelope system. Even the "electronic envelope" systems described above suffer from an inability to transmit data bidirectionally between parties except when all "transmitting" parties have installed the same cryptographic software onto their computers.

SUMMARY OF THE INVENTION

According to the present invention, there is provided to the user, the ability to send an "electronic envelope" across private and public communication networks including the use of e-mail. The sent information is protected from unauthorized access, corruption, tampering and theft while in transit and the "electronic envelope" allows the receiving user to decrypt the message without having to install any cryptographic software or hardware.

The invention includes a "secure reply" feature that allows the recipient of an encoded message to encrypt and return a message to the sender, again without having installed any cryptographic software. The present invention gives the receiver's reply the same level of protection and security that original encryption afforded the sender.

The present invention is also easier to use, only requiring the two participants to exchange keys (known as "passphrases") by any of the available modes of communication, such as a telephone conversation, postal mail, in person communication, or any other mode. Keys can be changed regularly, thereby enhancing security.

Not all users in an information exchange are required to install the systems of the present invention. For example, in a system where a service vendor was sending invoices (via e-mail) to selected customers, those customers would not need to install any cryptographic software. The present invention would provide all the necessary functionality to allow the secure return of payment instructions to the vendor. The same system using S/MIME or any of the other, prior art systems, would require all users to exchange keys with the vendor and obtain compatible software.

Imagine two people from different companies who need to communicate

securely, for example, Alice, who works for Widget Manufacturing Corporation (WMC), and Bob, an employee of WidgetBits, Inc., a supplier of components needed in the manufacture of widgets. Alice needs a proposal from Bob to supply WMC with widget components over the next 6 months.

Since the market for widgets is such a competitive environment, both Alice and Bob are keenly aware of the potential damage to their respective businesses should their competitors gain access to the information contained either in Alice's request or Bob's reply. Accordingly, they could use the system of the present invention to conduct their business.

Alice starts by creating a "request for proposal" (RFP) document using any word processor. She then uses the present invention to encrypt her document which "wraps" it in a self-decrypting "envelope". She also enables a feature to give Bob the ability to encrypt his reply. Lastly, she transmits this "envelope" to Bob using any means she chooses - e-mail, file transport, or copying the file to disk and mailing it, to name a few.

To continue with the "envelope" analogy, when Bob receives the encrypted message, ("envelope") he opens it using the previously received "passphrase". The document is then decrypted. Bob is assured that no one has seen the document while it was in transit and that is was not corrupted or modified in any way.

Bob is now free to write his proposal. Again, using any word processor, he creates a document to send to Alice as his reply. When the document is ready, he once again opens the original "envelope" and supplies the passphrase. The option to create a secure reply is offered. If selected, the proposal is encrypted using the same passphrase that allowed decryption of the original message. Bob is then free to transmit his proposal back to Alice as a secure reply file using any means at his disposal.

Upon receiving the secure reply, Alice decrypts it using the original encryption-decryption program of the present invention together with the original passphrase. She can now read Bob's proposal and continue to conduct her business.

Another example in which the present invention can be used is an implementation of a billing and payment processing system employed in an Electronic Commerce environment. A system of this type would use the ability to provide a secure reply for a more specialized purpose and so would implement a different user interface than in the preferred embodiments of the present invention. Nevertheless, the ability to provide a secure reply is unchanged.

In a (very simplified) electronic billing and payment system, the two

parties correspond via an e-mail connection. Both parties would first agree to a pass word or phrase (which may also be a Personal Identification Number or "PIN") with which the data being transferred is cryptographically secured. The vendor sends the customer an invoice or statement reflecting customer activity and an amount due. The customer responds with payment instructions and an authorization.

For example, the vendor would prepare a statement. This statement would then be encrypted and enclosed in an "envelope" along with a special purpose program designed to gather the customer's payment instructions. This envelope is transmitted through e-mail to the customer. The customer opens the envelope using the pass word or phrase established by prior agreement with the vendor. Once the contents of the envelope are decrypted, the statement is presented to the customer.

When the customer is ready to make a payment to the vendor, the envelope is again opened and the special purpose program automatically executes, presenting the customer with various payment options. When the customer has selected a payment method, a secure reply is generated (the payment selection program having automatically requested a secure reply from the original envelope).

The secure reply is then e-mailed back to the vendor. When the vendor receives the customer's secure reply, an automated process decrypts the reply, extracts the customer's payment instructions and submits them for further processing. A working implementation of this electronic billing and payment system exists in proprietary products of the assignee of the present invention.

The purpose of providing a secure reply feature is to allow two computer users to communicate securely (i.e. using encrypted data files) in circumstances where only one of them has the cryptographic software needed. Whatever software is needed to both decrypt the sent message as well as encrypt the reply is transmitted with the original message.

A secure reply may also be used in any circumstance where all that is needed is an acknowledgment that the message has been received and correctly decrypted since a secure reply cannot be created without knowledge of the correct pass word or phrase. In addition, it may be that the contents of the acknowledgment itself may be useful to a rival business or individual and so the encrypted reply provides the necessary security.

A working implementation of this electronic billing and payment system exists in proprietary products of the assignee of the present invention. The purpose of providing a secure reply feature is to allow two computer users to

communicate securely (i.e. using encrypted data files) in circumstances where only one of them has the cryptographic software needed. Whatever software is needed to both decrypt the sent message as well as encrypt the reply is transmitted with the original message.

For a different example, in an increasingly complex world it often become necessary for experts in diverse fields or specialties to work together in confidence. Many times these people must cooperate with little or no advanced notice and the information to be exchanged is of a sensitive or secret nature. All parties would like to execute an information exchange with a minimum of overhead expenditure.

Imagine, for example, a law firm (XYZ Partners) represents a well known party in contentious litigation. All the materials pertaining to this case are considered highly sensitive. Nevertheless, XYZ needs to consult with lawyers at another, distantly located firm (HIJ) specializing in an one area of the case. Time is, of course, of the essence.

Using the present invention, lawyers at XYZ can send documents to HIJ securely through the public e-mail network. The lawyers at HIJ can then edit any document sent or add their own input to the document and, using the present invention, reply to XYZ with the same level of security.

All parties are protected by the secure transmission and the collaborative effort requires a minimum of overhead and preparation.

Accordingly, it is an object of the present invention to provide a method and apparatus to send an encrypted message which permits an encrypted acknowledgment that a secure document had been successfully received and decrypted without special hardware or software at the site of the recipient.

It is an additional object to retrieve a secure document from a remote computer user by first sending an encrypted transmission with a dummy file.

It is a yet another object to foster a secure cooperative work environment by allowing two computer users to cooperatively develop a document such as a proposal, business plan, computer software, mechanical schematic, or the like. The document would be sent from the first user to the second using an protected transmission and the second user could then make any needed modifications to the document and return it using the present invention.

Yet another object of the invention is to enable the secure distribution of software with user registration information being returned using the present invention.

A further object of the invention is to permit the distribution of information about a product under development to a restricted group of computer users. Those users could respond with comments, suggestions, etc.

in accordance with the present invention.

The novel features which are characteristic of the invention, both as to structure and method of operation thereof, together with further objects and advantages thereof, will be understood from the following description, considered in connection with the accompanying drawings, in which the preferred embodiment of the invention is illustrated by way of example. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only, and they are not intended as a definition of the limits of the invention.

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1 is flow diagram showing the principles of operation of the present invention.

FIG. 2, including FIGS. 2a-2d, inclusive are flow charts of the steps taken in implementing the sending, receipt and return of secure information;

FIG. 3, including FIGS. 3a - 3d, inclusive is a more detailed flow chart of the process of the present invention; and

FIG. 4 including FIGS. 4a - 4b is a flow chart of an embodiment of the present invention for secure billing and payment transactions.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following Program Flow descriptions and diagrams describe the present invention as currently implemented by the assignee in a product offered by the applicant under the trademark Envelope98™ which is a secure transmission product. The same procedures apply in other situations with slight changes to the user interface.

Starting with FIG. 1, there is shown a generalized overview illustrating the present invention in use. Utilizing a specialized program, a message (envelope.exe) which includes an executable program and encrypted files is created which, when received and executed, decrypts the information contents upon the presentation of a preselected pass word or phrase. The entire message can be sent to a receiver using e-mail, a modem to modem file transfer over telephone lines, or may be recorded upon a disk which can be sent by courier or through the mails.

At the receiving end, the receiving party executes the program (envelope.exe) that is an integral part of the message. The receiving computer then asks for the agreed upon pass word or phrase and, upon its provision, operates upon the encrypted files to decrypt them. The receiver is then

given the option to provide a secure encrypted reply.

If the option is selected, after a reply is prepared, the received message is executed again and the reply option, when invoked, encrypts the reply message and the reply can be transmitted back to the originator using any of the same methods that could be employed in sending the initial message. Once the originator receives the message, his equipment permits a decryption of the returned file.

As shown in FIG. 1, the initial step is the creation of the envelope.exe file 12, which is explained in greater detail in connection with FIG. 2, below. In FIG. 1, the global computer network is used to transmit the file 12 in the transmitting step 14. At the recipient's end, the file is received 16 and the transmitted program is executed 18. If the recipient desires to proved an encrypted reply, the received program enables the preparation of the reply 20 and this reply is returned 22 through the global computer network. The reply is received by the original sender 24 who possesses the program to decrypt the reply 26.

In FIG. 2a, a preferred embodiment of the present invention is detailed, explaining the layout of the message which is to be transmitted. Initially, the user determines which files are to be transmitted, the encryption algorithm and pass word or phrase, whether to include the secure reply option, any other user-specified information and a name for the file. In the next step, the decrypt engine code is written and is attached to the other file elements.

Each file that is to be transmitted is sequentially retrieved and, if the option is selected, compressed. Next, special data is computed and in a successive step is encrypted using an algorithm that is user determined. A file header is prepared and the file is set for transmission.

Each of the remaining selected data files, is, in turn, processed through the same steps until all selected files have been compressed (if the option has been selected) provided with error detection codes, file size information and any other information which must be added and encrypted.. After all of the files are processed, the message is closed and is ready for transmission by any available means including the global computer network, modem to modem direct transmission, or storing on transportable media and forwarded by mail or courier.

With reference now to FIG. 2b, the steps performed at the receiving end are outlined. When the transmitted program is executed (envelope.exe), the envelope header is read and the information relative to the number of files transmitted is noted.

The various user instructions are then acted upon including the designation of the files to be extracted, the destination on the recipient's computer, pass word or phrase, the files, if any, to be included in a reply and, if a reply is to be made, the destination of the reply.

Next, each of the transmitted files is, in turn, decrypted, decompressed, is verified through an integrity check and written to the preselected destination in the recipient's system. If a secure reply is to be made, the next steps are to be found in FIG. 2c.

After the message is received and if the receiving party is ready to send a reply, the user again executes the received program (i.e. runs the envelope.exe instruction). The program is aware (through the use of a flag in the message header) that the original contents have already been decrypted and asks the user if a secure reply is to be created.

If the user requests a reply, the program asks for the name of the file or files to encrypt and, after encrypting the files, "wraps" them in a reply header. Notice that no decryption program is returned with the reply as it is a precondition of creating the message that the software needed to decrypt the reply is present.

If the secure reply option was provided and elected, the user determines which files to send, a file name, a password or pass phrase and a header. The received program, when executed again compresses (if desired) each file that is to be returned, special information is collected and each file is encrypted by the program which was transmitted to the recipient, who has no other encryption or decryption software available to his system. When all the files to be returned have been processed, the file is closed and the reply message is returned.

The steps to be followed when the reply is received at the original sender's location are indicated in FIG. 2d. The original sender's program can read the header of the reply and extract all of the necessary processing information. The original recipient's reply instructions are then processed which include the files to be extracted, the pass word or phrase and the destination of the transmitted files.

In turn, each returned file is decrypted using the appropriate algorithm. The file is next decompressed, if necessary. The contents are checked for integrity and the file is stored in the selected destination. When all files have been stored, the program is deemed complete.

Turning to FIG. 3a, the process at the receiving end is illustrated in a branching flow diagram. At the start, there is a choice of having a reply option on the command line. If no file name is present, a flag is set

indicating that a reply is to be created and a file name is generated. The program will then ask for the previously agreed upon pass word or phrase. Once provided, a crypt key is generated from the pass word or phrase and the message can be opened and read. After the header is read, the program checks to see if the reply option is indicated by a set flag but the message has not yet been decrypted. If so, a warning is given and the option to continue is offered. If the choice is not to continue, the program is exited.

Referring to FIG 3b, if the process is to continue, the next branch point is if the flag is not set but the message has been decrypted. If affirmative, the user is requested to decide if a reply is desired. If no reply is desired, the flag is cleared. If a reply is desired, the flag is set.

The next branch point examines the flag. If it is set, the key is verified, If not, the message is decrypted and the program is exited. The key is verified and if correct, the next check is made. If the key is not correct, the program exits. The next step is to check the reply file name. If one is not yet set, a name is acquired from the user. If there is a name set, a check is made to see if the file is accessible.

The process continues with reference now to FIG. 3c. A name is created for the reply output file. The user is asked if the created name is acceptable. If not, an acceptable file name is acquired. If so, it must be determined whether the file can be created. If not, the program is exited. If it can, the file is encrypted, a header is written for the "envelope" and the datafile and a message is displayed that the process has been completed.

Turning now to FIG. 3d, the process at the original message source is not reviewed with the receipt of the reply message. Because the original operating program is at this source, the reply can be immediately opened and read. The header identification is noted and the pass word or phrase is supplied. The crypt key is created from the pass word or phrase and the file name for the decrypted output file is supplied. If the key being used is incorrect, the program is exited. If correct, the datafile is decrypted and verified as being correct and uncorrupted. If it is not, an error message is displayed and the program is exited. If it is correct, then the program is exited without the error message.

An alternative embodiment of the present invention is illustrated in the flow diagram of FIG. 4 which includes FIGS. 4a and 4b. In this embodiment, a simplified program is illustrated for secure billing and payment. The bill is presented to the software program which compresses the bill, encrypts it and creates a secure "envelope". A e-mail message is created

which includes the encrypted bill. The e-mail server then sends the bill through the global computer network, sometimes calles the Internet,

Turning now to FIG. 4b, the message including the bill is received and the attachment is opened. A browser is launched which fetches, using the global computer network, a decryption program from a web site server specially authorized to perform this service. Once obtained, the decryption program is run.

The recipient is prompted for a Personal Identification Number ("PIN") or pass word or pass phrase. The PIN is checked for validity. If invalid, it is printed out and the program is shut down. If valid, the program then decrypts the message and sends a confirmation over the global network to the sender. The bill is then displayed in the browser window and a connection is arranged to a billing website. At this point, a payment authorization can be sent or the billing website can furnish other bill paying options. The biller website can be a neutral service provider or a financial institution which can be authorized to pay all or a portion of the bill or otherwise meet the payment responsibility.

Thus there has been described a system in which secure messages can be transmitted and secure replies can be created by the recipient without the need for any special software programs installed at the recipient's computer. The secure message includes a program, which when executed, enables a viewing of the received message and the preparation of a secure reply. However, the recipient cannot use the program to create new, secure messages to third parties or to permit those third parties to create secure replies.

The system of the present invention lends itself to the secure exchange of data or for secure financial transactions in which bills can be presented and paid. In one embodiment, any means of communication may be employed including, but not limited to the delivery of portable media. In an alternative embodiment, the transmitted program can be abbreviated so that a link is created through the global computer network that supplies the software necessary to decrypt the message and create the secure reply. Further a separate link can be created with a secure financial services site that can handle a financial transaction based on the submission of a secure billing.

The scope of the invention should be limited only by the scope of the claims attached below.

CLAIMS

1. A method for the secure transmission of documents comprising the steps of:

using a security program at a sending location for creating an encrypted file including an executable program with the document;

transmitting said encrypted file to a remote recipient;

receiving said encrypted file at a location lacking said security program;

executing, at the receiving location, the received said executable program; and

decrypting said received file using said received program.

2. The method of Claim 1, further including the steps of:

including a pass phrase as a part of said executable program to prevent unauthorized decryption of the received said encrypted file.

3. The method of Claim 2, further including said pass phrase in the encryption algorithm used in the creation of said encrypted file.

4. The method of Claim 1, wherein said executable program includes, as a step when running, a verification step for confirming the integrity of the received file.

5. The method of Claim 1, wherein the step of creating includes a file compression step prior to the encryption of said file.

6. The method of Claim 1, further including a secure reply option comprising the steps of:

providing, in said executable program, a option for a secure reply;

electing, at said receiving end, the secure reply option;

using said received executable program to create a secure reply file similar to that created by the security program at the transmitting end;

transmitting said secure reply file from said remote location to said sending location; and

using said security program at said sending location to decrypt said secure reply file,

whereby a receiving location lacking a security program can receive secure messages and send secure replies.

7. The method of Claim 6, further including the steps of including a pass phrase in the creation of said secure file and wherein said received

executable program requires said pass phrase for execution of said transmitted program.

8. The method of Claim 6, further including the step of verifying the integrity of said secure reply file at said transmitting location.

9. Apparatus for the secure transmission of documents comprising:
creating means including a security program at a sending location for creating an encrypted file incorporating an executable program with the document;
means for transmitting said encrypted file to a remote recipient;
means for receiving said encrypted file at a location lacking said security program;
means for executing, at the receiving location, the received said executable program; and
means responsive to the running of said executable program for decrypting said received file.

10. The apparatus of Claim 9, further including:
means for including a pass phrase as a part of said executable program to prevent unauthorized decryption of the received said encrypted file.

11. The apparatus of Claim 10, wherein said creating means include said pass phrase in the encryption algorithm used in the creation of said encrypted file.

12. The apparatus of Claim 9, wherein said means for executing include, verification means for confirming the integrity of the received file.

13. The apparatus of Claim 9, wherein said creating means include compression means for compressing a file prior to the encryption of said file.

14. The apparatus of Claim 9, further including means for creating a secure reply comprising:
selecting means in said executable program for choosing a secure reply;
means at said receiving end for creating a secure reply including means responsive to said received executable program for creating a secure reply file similar to that created by the security program at the transmitting end;
means at said remote location for transmitting said secure reply file from said remote location to said sending location; and
means for executing said security program at said sending location to

decrypt said secure reply file,
whereby a receiving location lacking a security program can receive secure messages and send secure replies.

15. The apparatus of Claim 14, further including means for including a pass phrase in the creation of said secure file and wherein said received executable program is responsive to said pass phrase for execution of said transmitted program.

16. The apparatus of Claim 14, wherein said means for executing include means for verifying the integrity of said secure reply file at said transmitting location.

17. A method for the secure transmission of documents comprising the steps of:

using a security program at a sending location for creating an encrypted file including an executable program with the document;

transmitting said encrypted file to a remote recipient;

receiving said encrypted file at a location lacking said security program;

executing, at the receiving location, the received said executable program;

connecting to a predetermined site on a global computer network;

retrieving from said predetermined site a suitable executable program for decrypting said received encrypted file and

decrypting said received file using said retrieved program.

18. The method of Claim 17, further including the steps of:

including a pass phrase as a part of said executable program to enable said predetermined site to download said suitable executable program thereby preventing unauthorized decryption of the received said encrypted file.

19. The method of Claim 18, further including said pass phrase in the encryption algorithm used in the creation of said encrypted file.

20. The method of Claim 17, wherein said suitable executable program includes, as a step when running, a verification step for confirming the integrity of the received file.

21. The method of Claim 17, wherein the step of creating includes a file compression step prior to the encryption of said file.

22. The method of Claim 17, further including a secure reply option

comprising the steps of:

providing, in said suitable executable program, a option for a secure reply;

electing, at said receiving end, the secure reply option;

using said received suitable executable program to create a secure reply file similar to that originally created by the security program at the transmitting end;

transmitting said secure reply file from said remote location to said sending location; and

using said security program at said sending location to decrypt said secure reply file,

whereby a receiving location lacking a security program can receive secure messages and send secure replies.

23. The method of Claim 22, further including the steps of including a pass phrase in the creation of said secure file and wherein said received executable program requires said pass phrase for acquisition of said suitable executable program.

24. The method of Claim 22, further including the step of verifying the integrity of said secure reply file at said transmitting location.

25. Apparatus for the secure transmission of documents comprising:

creating means including a security program at a sending location for creating an encrypted file incorporating an executable program with the document;

means for transmitting said encrypted file to a remote recipient;

means for receiving said encrypted file at a location lacking said security program;

means for executing, at the receiving location, the received said executable program;

means responsive to the running of said executable program for contacting a predetermined site on the global computer network for retrieving a suitable executable program for decrypting said received file.

26. The apparatus of Claim 25, further including:

means for including a pass phrase as a part of said executable program to enable communication with said predetermined site to authorize downloading of said suitable executable program and to prevent unauthorized decryption of the received said encrypted file.

27. The apparatus of Claim 26, wherein said creating means include said pass phrase in the encryption algorithm used in the creation of said

encrypted file.

28. The apparatus of Claim 25, further including means for running said suitable executable program wherein said means for running include verification means for confirming the integrity of the received file.

29. The apparatus of Claim 25, wherein said creating means include compression means for compressing a file prior to the encryption of said file.

30. The apparatus of Claim 25, further including means for creating a secure reply comprising:

selecting means in said suitable executable program for choosing a secure reply;

means at said receiving end for creating a secure reply including means responsive to said received suitable executable program for creating a secure reply file similar to that created by the security program at the transmitting end;

means at said remote location for transmitting said secure reply file from said remote location to said sending location; and

means for executing said security program at said sending location to decrypt said secure reply file,

whereby a receiving location lacking a security program can receive secure messages and send secure replies.

31. The apparatus of Claim 30, further including means for including a pass phrase in the creation of said secure file and wherein said received executable program is responsive to said pass phrase for downloading said suitable executable program.

32. The apparatus of Claim 30, including means for executing said suitable executable program, said suitable executable program including means for verifying the integrity of said secure reply file at said transmitting location.

33. The method of Claim 17, further including a reply option comprising the steps of:

providing, in said suitable executable program, a option for a reply;

electing, at said receiving end, the reply option;

using said received suitable executable program to contact a second, predetermined global computer network site; and

instructing said second global computer network site to take a selected

action;
whereby a receiving location lacking a security program can receive secure messages and send instructions to a selected global computer network site.

34. The method of Claim 33, further including the steps of including a pass phrase in the creation of said secure file and wherein said received executable program requires said pass phrase for acquisition of said suitable executable program.

35. The method of Claim 33 further including the step of sending a receipt confirmation to said sending location.

36. The method of Claim 33, further including the step of directing said selected second global computer network site to send a confirmation message to said sending location.

37. The apparatus of Claim 25, further including means for creating a reply comprising:

communicating means in said suitable executable program for contacting a second predetermined global communication network site;and

means at said remote location for transmitting a predetermined instruction to said second global computer network site.

38. The apparatus of Claim 37, further including means for transmitting a receipt confirmation to said sending location.

39. The apparatus of Claim 37, further including means for directing said second global computer network site to send a receipt confirmation to said sending location.

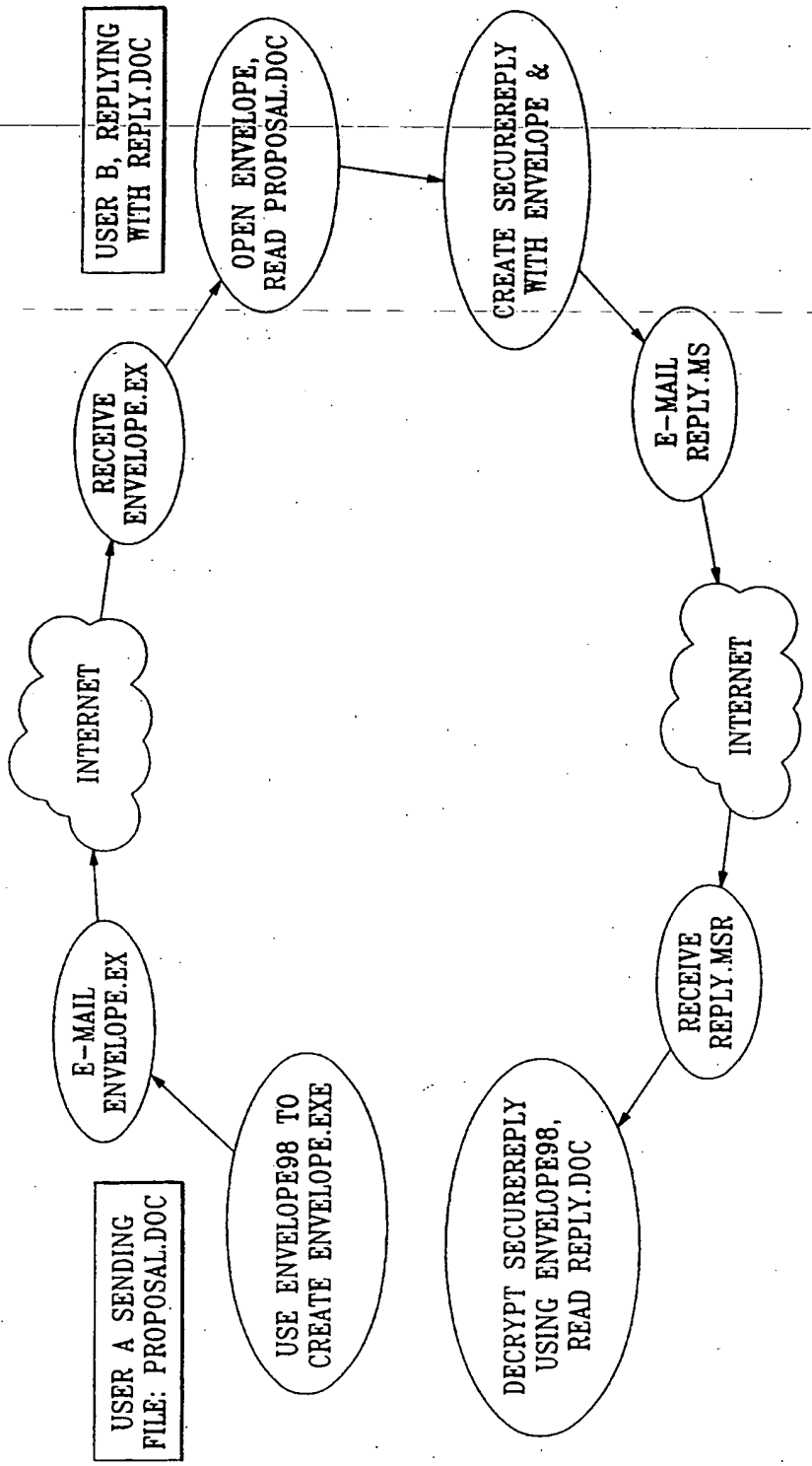

USER A SENDING FILE: PROPOSAL.DOC
USE ENVELOPE98 TO CREATE ENVELOPE.EXE
E-MAIL ENVELOPE.EX
INTERNET
RECEIVE ENVELOPE.EX
USER B, REPLYING WITH REPLY.DOC
OPEN ENVELOPE, READ PROPOSAL.DOC
CREATE SECUREREPLY WITH ENVELOPE &
E-MAIL REPLY.MS
INTERNET
RECEIVE REPLY.MSR
DECRYPT SECUREREPLY USING ENVELOPE98, READ REPLY.DOC

Fig. 1

FIG. 2a

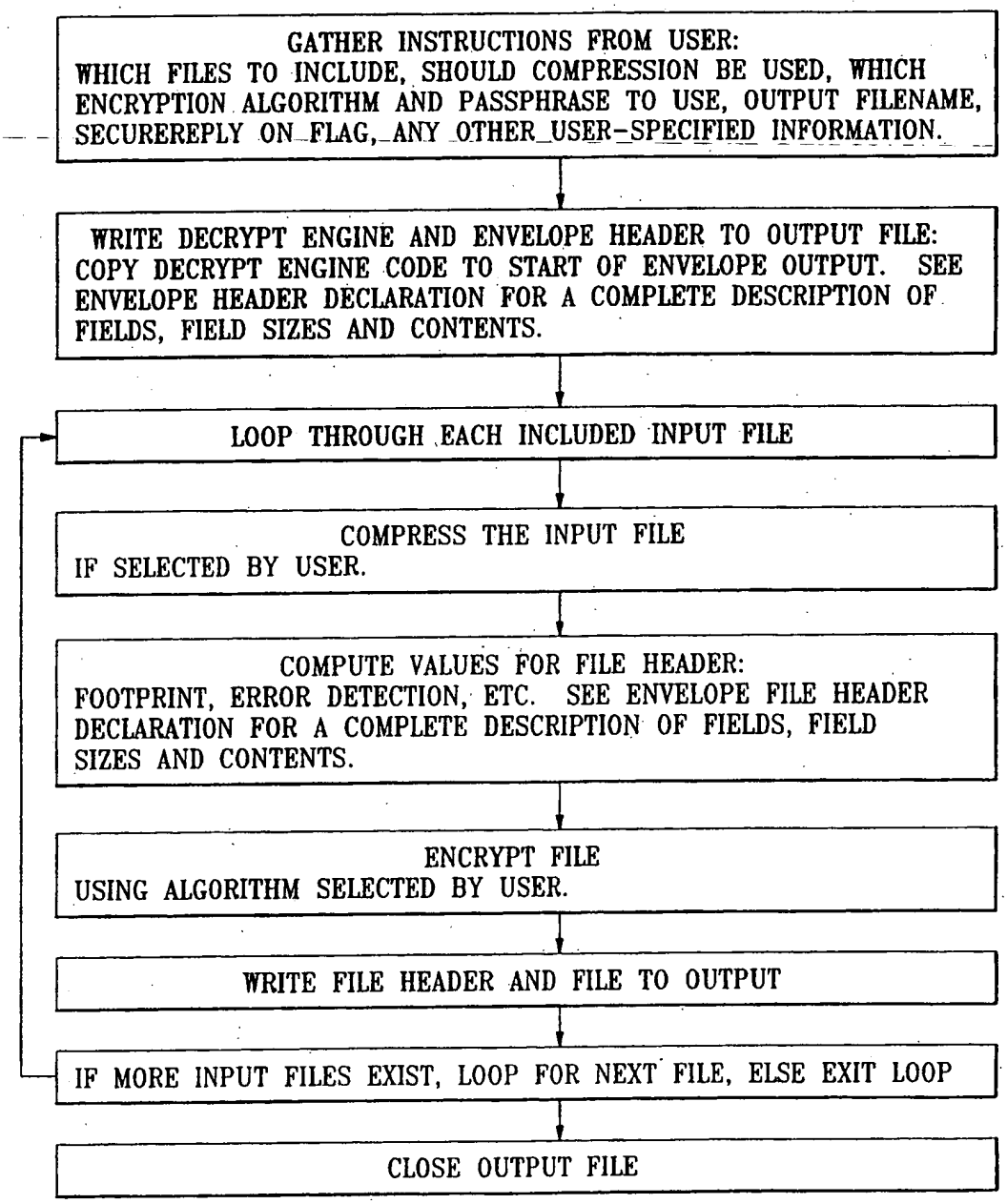

GATHER INSTRUCTIONS FROM USER:
WHICH FILES TO INCLUDE, SHOULD COMPRESSION BE USED, WHICH ENCRYPTION ALGORITHM AND PASSPHRASE TO USE, OUTPUT FILENAME, SECUREREPLY ON FLAG, ANY OTHER USER-SPECIFIED INFORMATION.
WRITE DECRYPT ENGINE AND ENVELOPE HEADER TO OUTPUT FILE:
COPY DECRYPT ENGINE CODE TO START OF ENVELOPE OUTPUT. SEE ENVELOPE HEADER DECLARATION FOR A COMPLETE DESCRIPTION OF FIELDS, FIELD SIZES AND CONTENTS.
LOOP THROUGH EACH INCLUDED INPUT FILE
COMPRESS THE INPUT FILE
IF SELECTED BY USER.
COMPUTE VALUES FOR FILE HEADER:
FOOTPRINT, ERROR DETECTION, ETC. SEE ENVELOPE FILE HEADER DECLARATION FOR A COMPLETE DESCRIPTION OF FIELDS, FIELD SIZES AND CONTENTS.
ENCRYPT FILE
USING ALGORITHM SELECTED BY USER.
WRITE FILE HEADER AND FILE TO OUTPUT
IF MORE INPUT FILES EXIST, LOOP FOR NEXT FILE, ELSE EXIT LOOP
CLOSE OUTPUT FILE

FIG. 2b

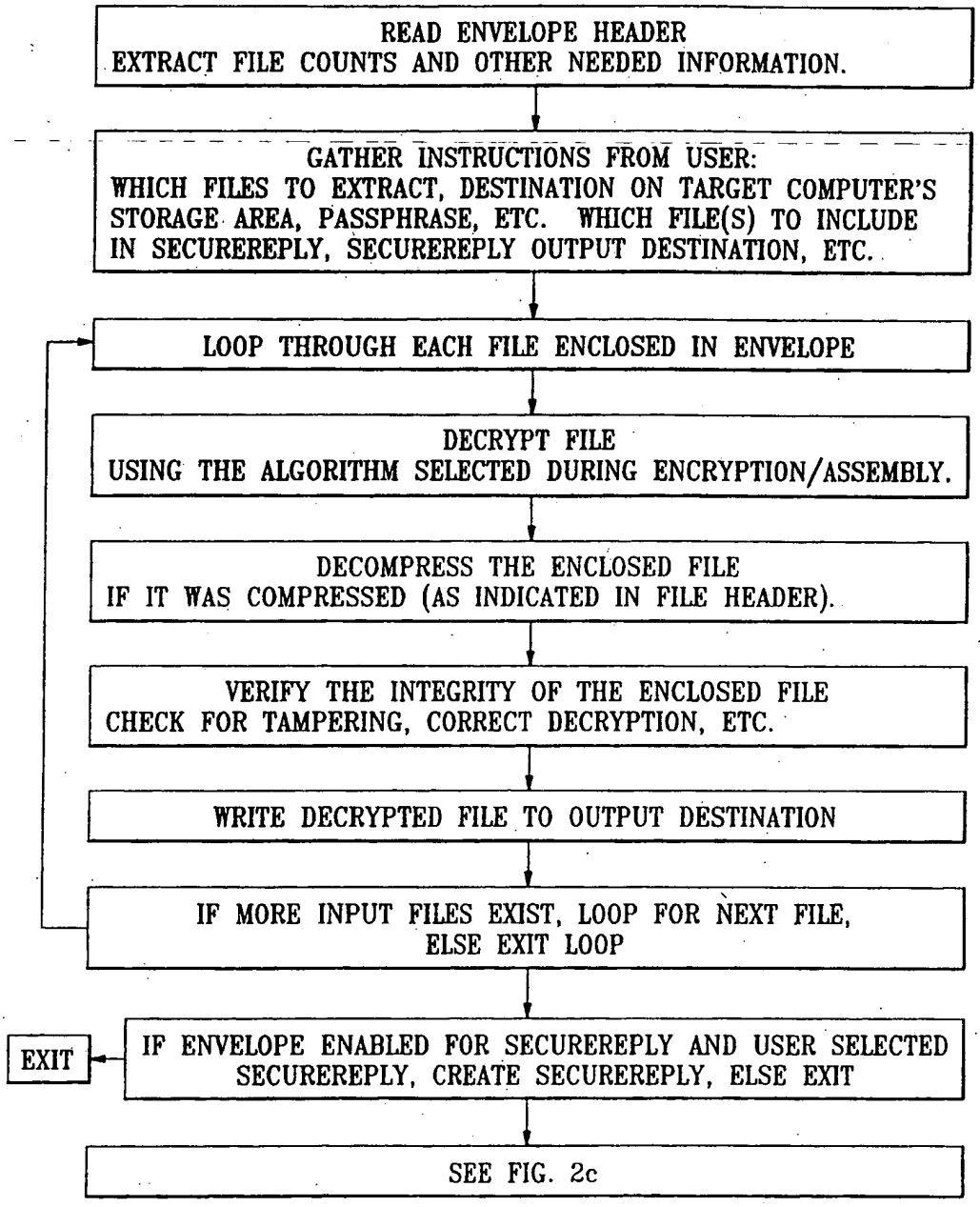

READ ENVELOPE HEADER
EXTRACT FILE COUNTS AND OTHER NEEDED INFORMATION.
GATHER INSTRUCTIONS FROM USER:
WHICH FILES TO EXTRACT, DESTINATION ON TARGET COMPUTER'S STORAGE AREA, PASSPHRASE, ETC. WHICH FILE(S) TO INCLUDE IN SECUREREPLY, SECUREREPLY OUTPUT DESTINATION, ETC.
LOOP THROUGH EACH FILE ENCLOSED IN ENVELOPE
DECRYPT FILE
USING THE ALGORITHM SELECTED DURING ENCRYPTION/ASSEMBLY.
DECOMPRESS THE ENCLOSED FILE
IF IT WAS COMPRESSED (AS INDICATED IN FILE HEADER).
VERIFY THE INTEGRITY OF THE ENCLOSED FILE
CHECK FOR TAMPERING, CORRECT DECRYPTION, ETC.
WRITE DECRYPTED FILE TO OUTPUT DESTINATION
IF MORE INPUT FILES EXIST, LOOP FOR NEXT FILE,
ELSE EXIT LOOP
EXIT
IF ENVELOPE ENABLED FOR SECUREREPLY AND USER SELECTED SECUREREPLY, CREATE SECUREREPLY, ELSE EXIT
SEE FIG. 2c

Fig. 2c

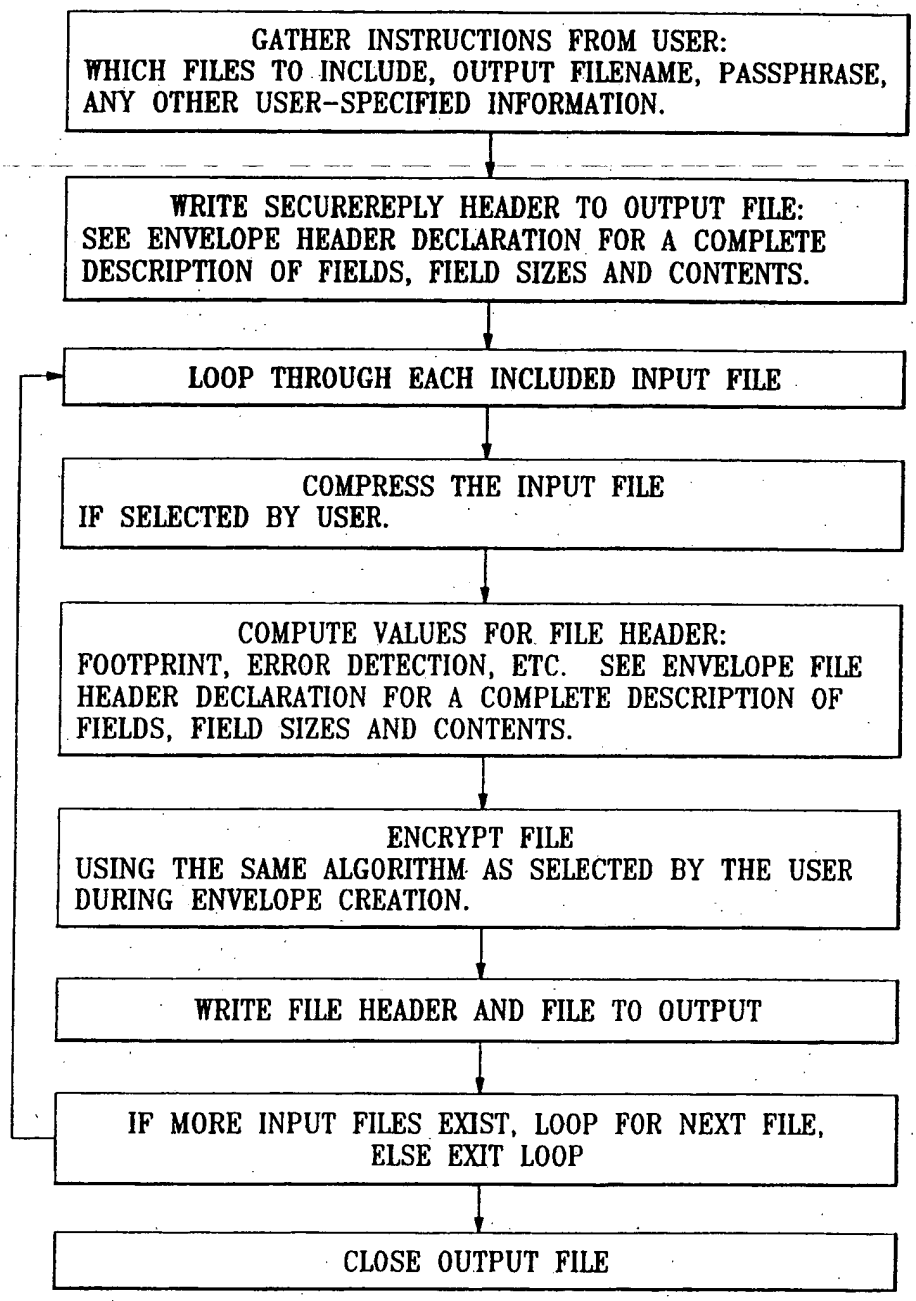
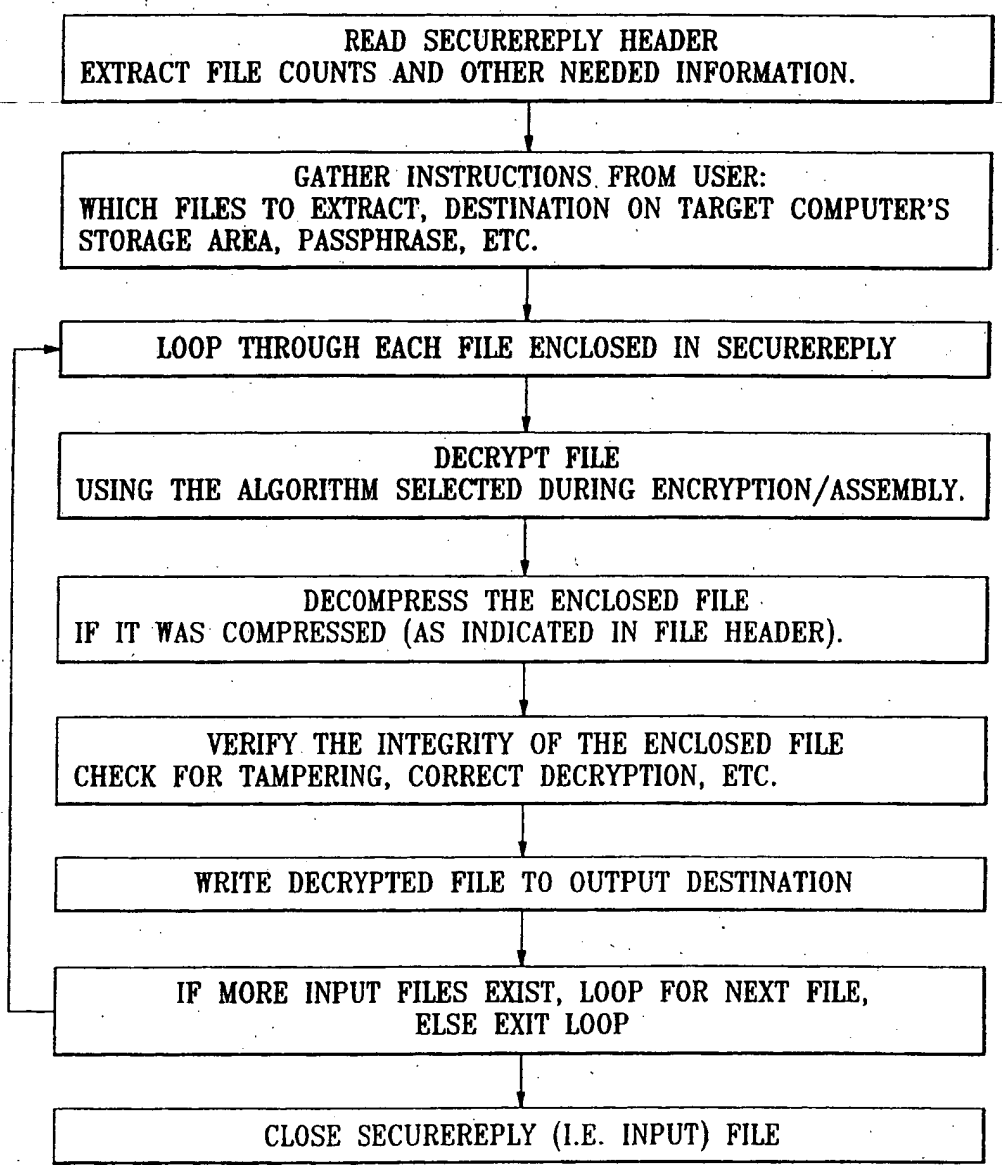

GATHER INSTRUCTIONS FROM USER:
WHICH FILES TO INCLUDE, OUTPUT FILENAME, PASSPHRASE,
ANY OTHER USER-SPECIFIED INFORMATION.
WRITE SECUREREPLY HEADER TO OUTPUT FILE:
SEE ENVELOPE HEADER DECLARATION FOR A COMPLETE
DESCRIPTION OF FIELDS, FIELD SIZES AND CONTENTS.
LOOP THROUGH EACH INCLUDED INPUT FILE
COMPRESS THE INPUT FILE
IF SELECTED BY USER.
COMPUTE VALUES FOR FILE HEADER:
FOOTPRINT, ERROR DETECTION, ETC. SEE ENVELOPE FILE
HEADER DECLARATION FOR A COMPLETE DESCRIPTION OF
FIELDS, FIELD SIZES AND CONTENTS.
ENCRYPT FILE
USING THE SAME ALGORITHM AS SELECTED BY THE USER
DURING ENVELOPE CREATION.
WRITE FILE HEADER AND FILE TO OUTPUT
IF MORE INPUT FILES EXIST, LOOP FOR NEXT FILE,
ELSE EXIT LOOP
CLOSE OUTPUT FILE

Fig. 2d


READ SECUREREPLY HEADER
EXTRACT FILE COUNTS AND OTHER NEEDED INFORMATION.
GATHER INSTRUCTIONS FROM USER:
WHICH FILES TO EXTRACT, DESTINATION ON TARGET COMPUTER'S STORAGE AREA, PASSPHRASE, ETC.
LOOP THROUGH EACH FILE ENCLOSED IN SECUREREPLY
DECRYPT FILE
USING THE ALGORITHM SELECTED DURING ENCRYPTION/ASSEMBLY.
DECOMPRESS THE ENCLOSED FILE
IF IT WAS COMPRESSED (AS INDICATED IN FILE HEADER).
VERIFY THE INTEGRITY OF THE ENCLOSED FILE
CHECK FOR TAMPERING, CORRECT DECRYPTION, ETC.
WRITE DECRYPTED FILE TO OUTPUT DESTINATION
IF MORE INPUT FILES EXIST, LOOP FOR NEXT FILE,
ELSE EXIT LOOP
CLOSE SECUREREPLY (I.E. INPUT) FILE

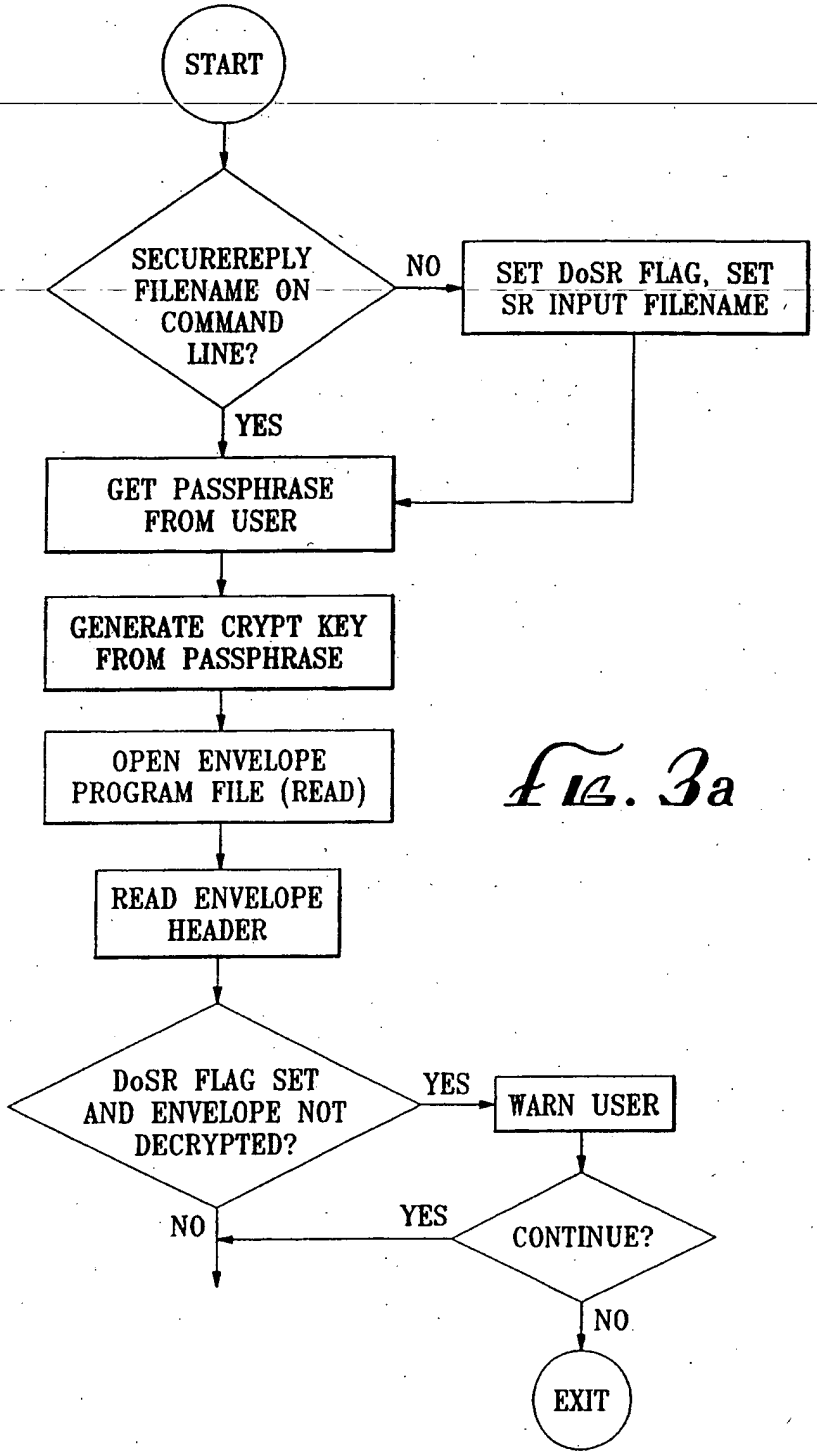

START
SECUREREPLY FILENAME ON COMMAND LINE?
NO
SET DoSR FLAG, SET SR INPUT FILENAME
YES
GET PASSPHRASE FROM USER
GENERATE CRYPT KEY FROM PASSPHRASE
OPEN ENVELOPE PROGRAM FILE (READ)
READ ENVELOPE HEADER
DoSR FLAG SET AND ENVELOPE NOT DECRYPTED?
YES
WARN USER
NO
YES
CONTINUE?
NO
EXIT

Fig. 3a

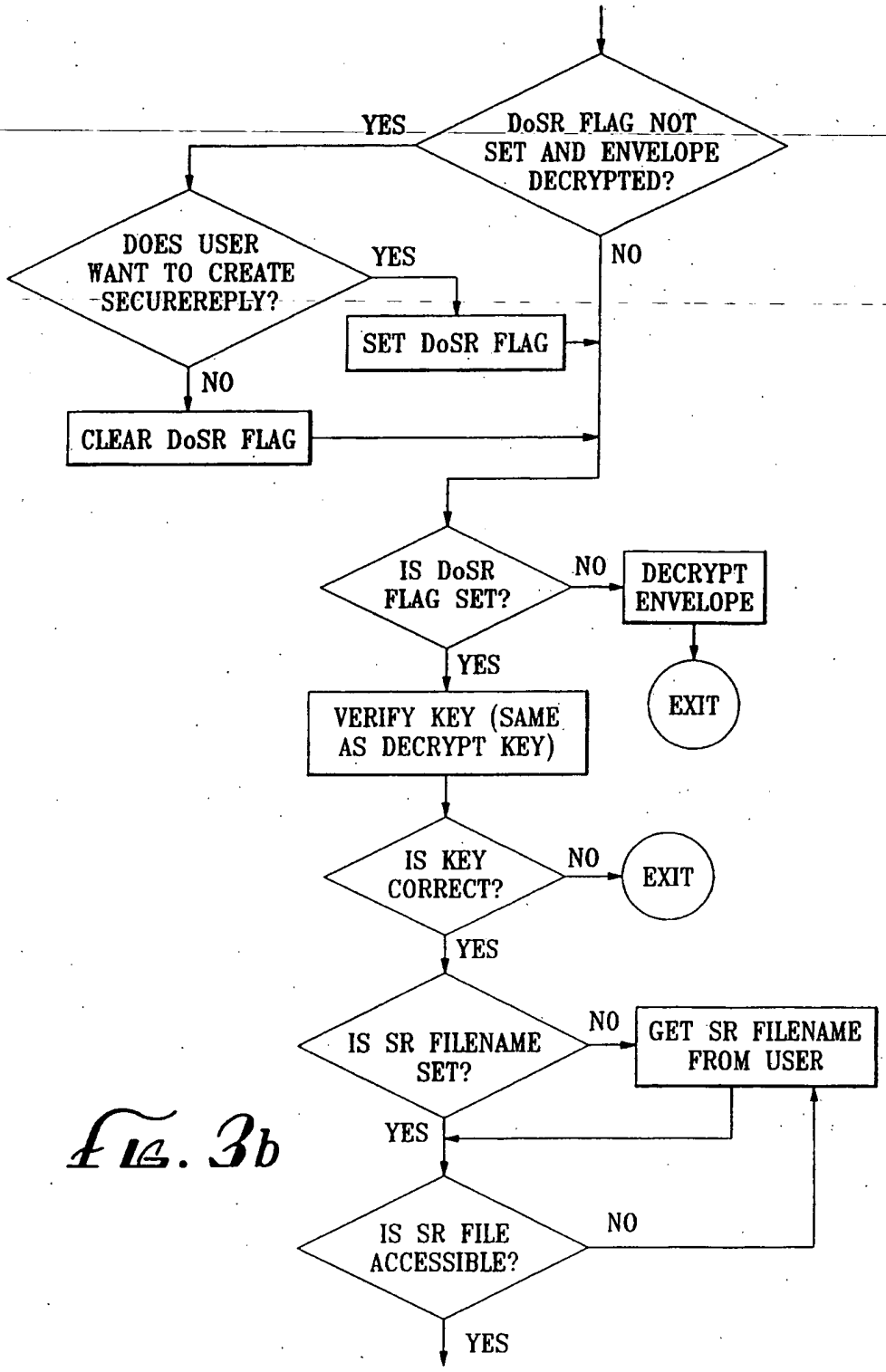

DoSR_FLAG_NOT SET AND ENVELOPE DECRYPTED?
YES
NO
DOES USER WANT TO CREATE SECUREREPLY?
YES
NO
SET DoSR FLAG
CLEAR DoSR FLAG
IS DoSR FLAG SET?
NO
DECRYPT ENVELOPE
EXIT
YES
VERIFY KEY (SAME AS DECRYPT KEY)
IS KEY CORRECT?
NO
EXIT
YES
IS SR FILENAME SET?
NO
GET SR FILENAME FROM USER
YES
IS SR FILE ACCESSIBLE?
NO
YES

Fig. 3b

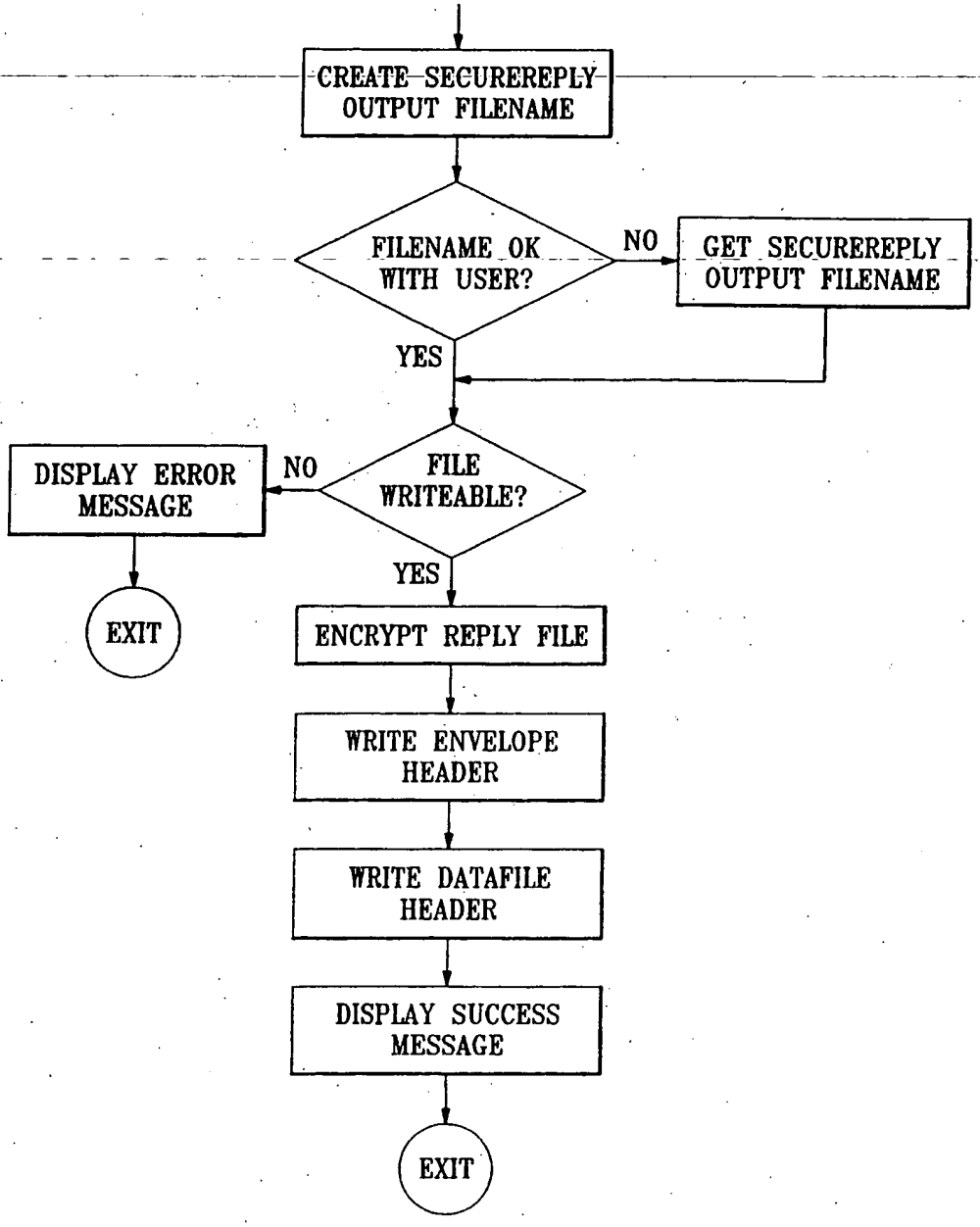

CREATE SECUREREPLY OUTPUT FILENAME
FILENAME OK WITH USER?
NO
GET SECUREREPLY OUTPUT FILENAME
YES
DISPLAY ERROR MESSAGE
NO
FILE WRITEABLE?
YES
EXIT
ENCRYPT REPLY FILE
WRITE ENVELOPE HEADER
WRITE DATAFILE HEADER
DISPLAY SUCCESS MESSAGE
EXIT

Fig. 3c

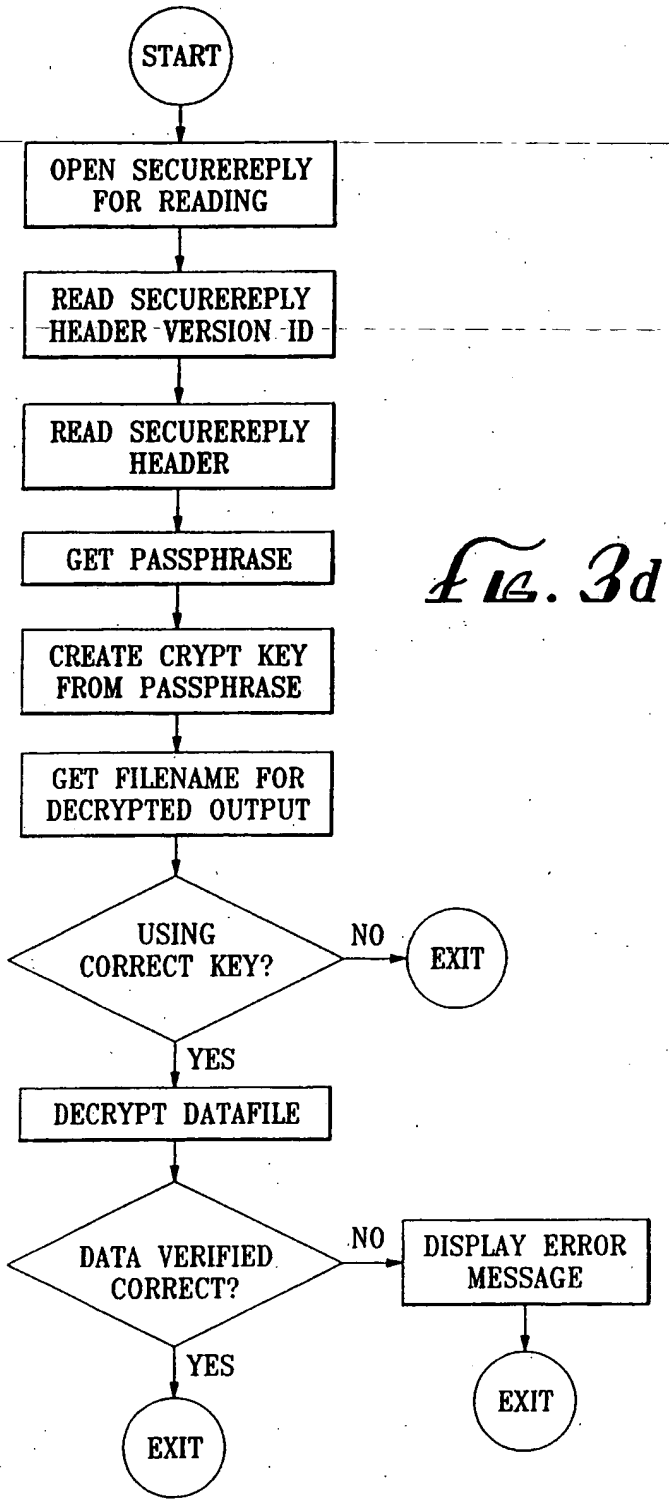

START
OPEN SECUREREPLY FOR READING
READ SECUREREPLY HEADER VERSION ID
READ SECUREREPLY HEADER
GET PASSPHRASE
CREATE CRYPT KEY FROM PASSPHRASE
GET FILENAME FOR DECRYPTED OUTPUT
USING CORRECT KEY?
NO
EXIT
YES
DECRYPT DATAFILE
DATA VERIFIED CORRECT?
NO
DISPLAY ERROR MESSAGE
YES
EXIT
EXIT

Fig. 3d

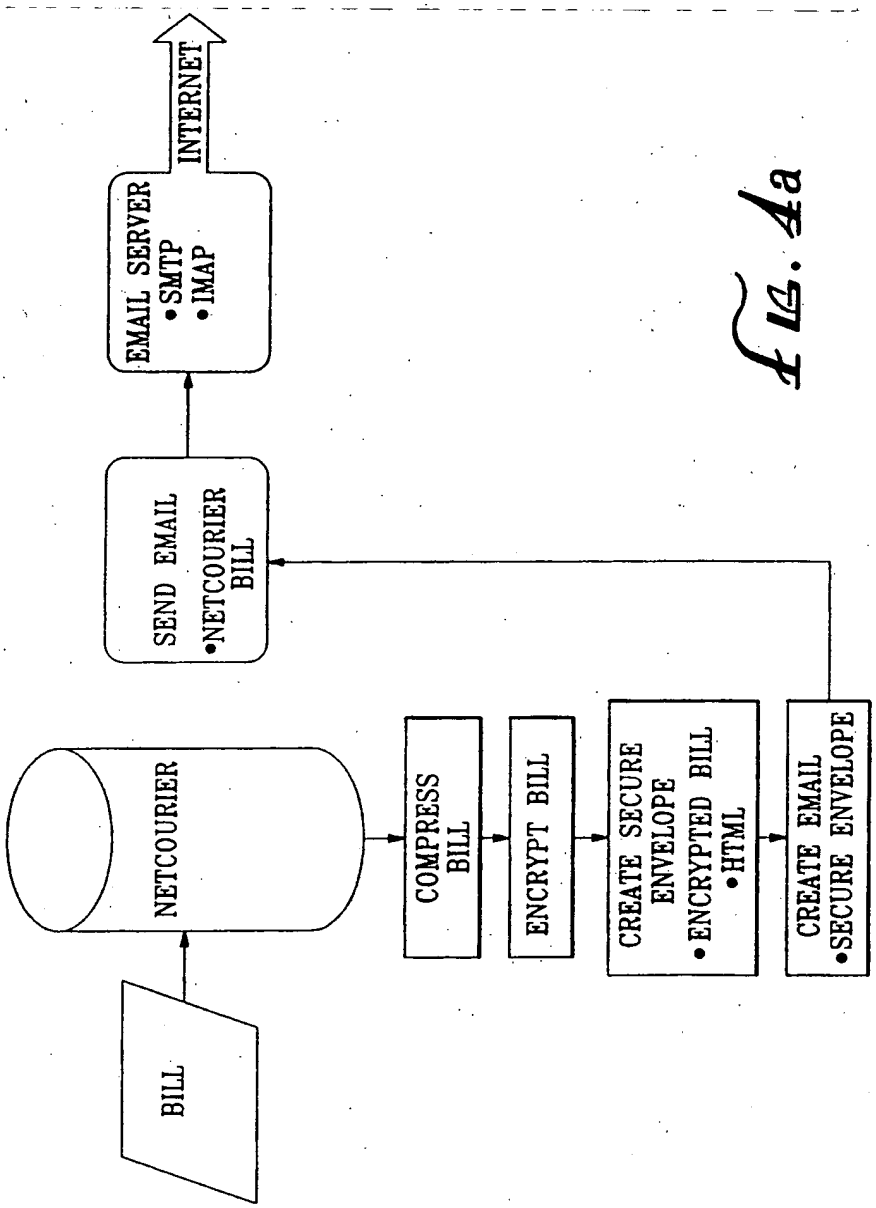

BILL
NETCOURIER
COMPRESS BILL
ENCRYPT BILL
CREATE SECURE ENVELOPE
• ENCRYPTED BILL
• HTML
CREATE EMAIL
• SECURE ENVELOPE
SEND EMAIL
• NETCOURIER BILL
EMAIL SERVER
• SMTP
• IMAP
INTERNET

Fig. 4a

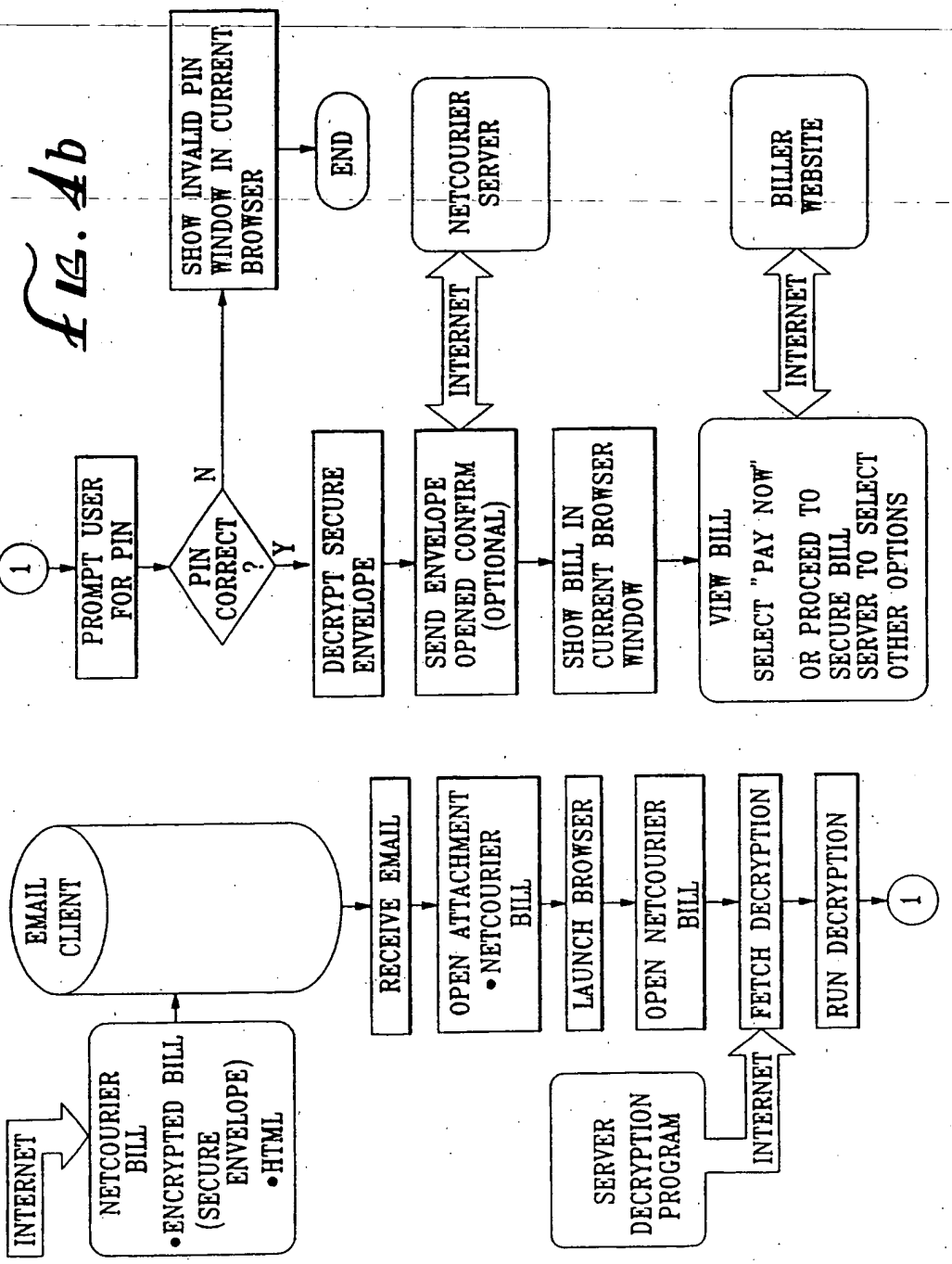

INTERNET
NETCOURIER BILL
•ENCRYPTED BILL (SECURE ENVELOPE)
•HTML
EMAIL CLIENT
RECEIVE EMAIL
OPEN ATTACHMENT
•NETCOURIER BILL
LAUNCH BROWSER
OPEN NETCOURIER BILL
SERVER DECRYPTION PROGRAM
INTERNET
FETCH DECRYPTION
RUN DECRYPTION
1
PROMPT USER FOR PIN
PIN CORRECT ?
N
Y
SHOW INVALID PIN WINDOW IN CURRENT BROWSER
END
DECRYPT SECURE ENVELOPE
SEND ENVELOPE OPENED CONFIRM (OPTIONAL)
INTERNET
NETCOURIER SERVER
SHOW BILL IN CURRENT BROWSER WINDOW
VIEW BILL
SELECT "PAY NOW"
OR PROCEED TO SECURE BILL SERVER TO SELECT OTHER OPTIONS
INTERNET
BILLER WEBSITE

Fig. 4b

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 00/07588

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 679 978 A (IBM) 2 November 1995 (1995-11-02) abstract page 2, column 1, line 31 - line 37 page 3, column 4, line 34 -page 4, column 5, line 23 page 14, column 25, line 8 -column 26, line 34 page 19, column 36, line 39 -page 20, column 37, line 14; claims 1-3 --- -/--	1-3, 9-11, 17-19, 25-27

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2000	21/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 00/07588

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 805 702 A (FOX CHRISTOPHER W ET AL) 8 September 1998 (1998-09-08) abstract column 1, line 29 - line 49 column 3, line 29 - line 46 column 4, line 37 -column 6, line 23	1-39

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/US 00/07588

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0679978 A	02-11-1995	CA 2143874 A	26-10-1995
		JP 7295799 A	10-11-1995
		KR 200445 B	15-06-1999
		US 5737416 A	07-04-1998
US 5805702 A	08-09-1998	AU 702508 B	25-02-1999
		AU 7374596 A	17-04-1997
		CA 2232791 A	03-04-1997
		CN 1198233 A	04-11-1998
		EP 1020821 A	19-07-2000
		EP 0862769 A	09-09-1998
		JP 11513509 T	16-11-1999
		WO 9712344 A	03-04-1997
		US 5748740 A	05-05-1998